

LA EXPERIENCIA DEL CENTRO CRIPTOLÓGICO NACIONAL

Firma electrónica con seguridad certificada

SEMINARIO “DOCUMENTACIÓN Y SEGURIDAD ELECTRÓNICA”

Revistas SOCINFO

17 de junio de 2008



Índice

- * **INTRODUCCIÓN**
- * **CONCEPTO DE SEGURIDAD**
- * **NORMATIVA RELATIVA A FIRMA ELECTRÓNICA**
- * **CERTIFICACIÓN DE DISPOSITIVOS-APLICACIONES DE FIRMA**
- * **CONCLUSIONES**

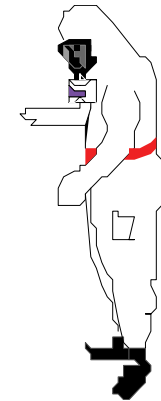
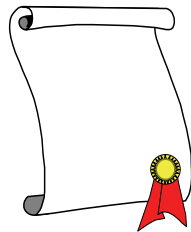
Introducción

- **EXPANSIÓN DE PRODUCTOS Y SERVICIOS BASADOS EN FIRMA ELECTRÓNICA.**
- **FACTORES QUE IMPULSARÁN ESTA EXPANSIÓN:**
 - **Implantación del DNI electrónico.**
 - **Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos.**
 - **Mayor uso de dispositivos móviles o personales.**

ES CONVENIENTE RECORDAR LA NORMATIVA E INCIDIR SOBRE DETERMINADOS ASPECTOS

Concepto de Seguridad

SEGURIDAD



Personal

Información

Material

Instalaciones

Actividad

**Seguridad
del personal**

**Seguridad de la
documentación**

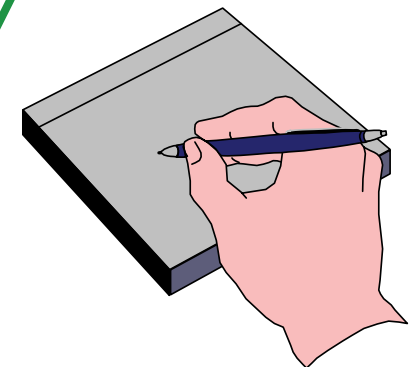
**Seguridad
de las TI**

“Si piensa que la tecnología puede resolver sus problemas de seguridad, entonces no entiende el problema y no entiende la tecnología”

B. Schneier (Secrets and Lies)

Concepto de Seguridad

- **Formación**
 - **Políticas**
 - **Procedimientos**
 - **Herramientas**
 - **Valoración > Acreditación**
 - **Evaluación > Certificación**
- Firma electrónica**



Normativa relativa a Firma Electrónica

DIRECTIVA 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica.

Ley 59/2003, de 19 de diciembre, de firma electrónica.

FIRMA ELECTRÓNICA

FIRMA ELECTRÓNICA AVANZADA: la firma electrónica que:

- está vinculada al firmante de manera única;
- permite la identificación del firmante;
- ha sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;
- está vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos es detectable.

Normativa relativa a Firma Electrónica

CERTIFICADO ELECTRÓNICO / CERTIFICADO ELEC. RECONOCIDO

DISPOSITIVO DE CREACIÓN DE FIRMA

DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA: un dispositivo de creación de firma que cumple los siguientes requisitos:

- los datos utilizados para la generación de firma pueden producirse sólo una vez y se garantiza razonablemente su secreto;
- existe la seguridad razonable de que los datos utilizados para la generación de firma no pueden ser hallados por deducción y la firma está protegida contra la falsificación mediante la tecnología existente en cada momento;
- los datos utilizados para la generación de firma pueden ser protegidos de forma fiable por el firmante legítimo contra su utilización por terceros;
- el dispositivo utilizado no altera los datos que deben firmarse ni impide que dichos datos se muestren al firmante antes del proceso de firma.

Normativa relativa a Firma Electrónica



Certificación de los **DISPOSITIVOS** de firma

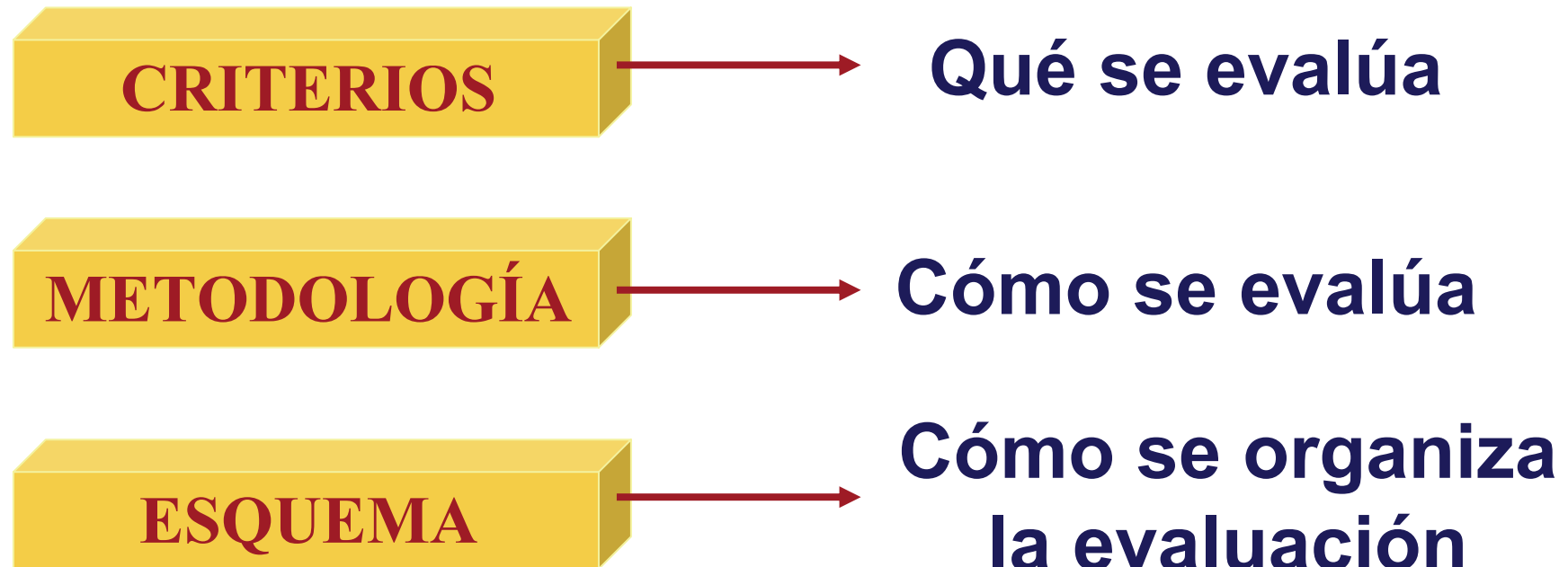
La conformidad de los dispositivos de creación de firma con los requisitos exigidos para ser considerados seguros se determina:

- Siguiendo un proceso de evaluación/certificación.
- Realizado por un organismo de certificación reconocido por una entidad de acreditación designada según lo establecido en la Ley 21/1992, de Industria.
- Utilizando las normas técnicas publicadas en el Diario Oficial de la Unión Europea = CWA14169.

Certificación de los **DISPOSITIVOS** de firma

EVALUACIÓN: Proceso en el que se contrasta la seguridad de un producto de TI.

CERTIFICACIÓN: Es la determinación, obtenida tras un proceso metodológico, de la *conformidad* del producto con unos requisitos preestablecidos.



Certificación de los DISPOSITIVOS de firma

CWA14169 (CEN Workshop Agreement)

- Decisión de la Comisión de 14 de julio de 2003.
- Define los requisitos de seguridad de los dispositivos seguros de creación de firma mediante Perfiles de Protección según los Criterios Comunes.

CRITERIOS

Common Criteria for Information Technology Security Evaluation (CC)

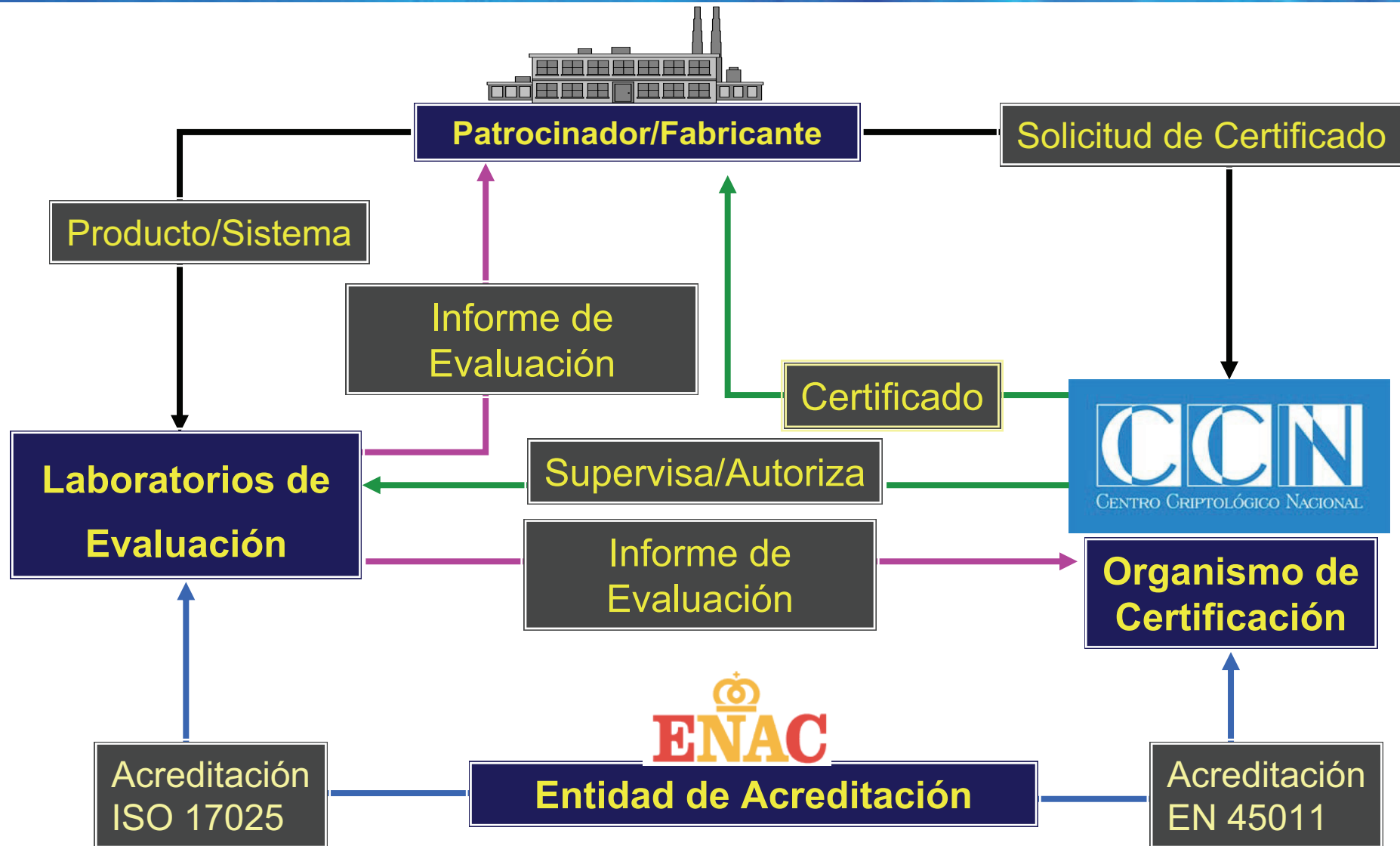
ISO/IEC 15408. Evaluation Criteria for IT Security

METODOLOGÍA

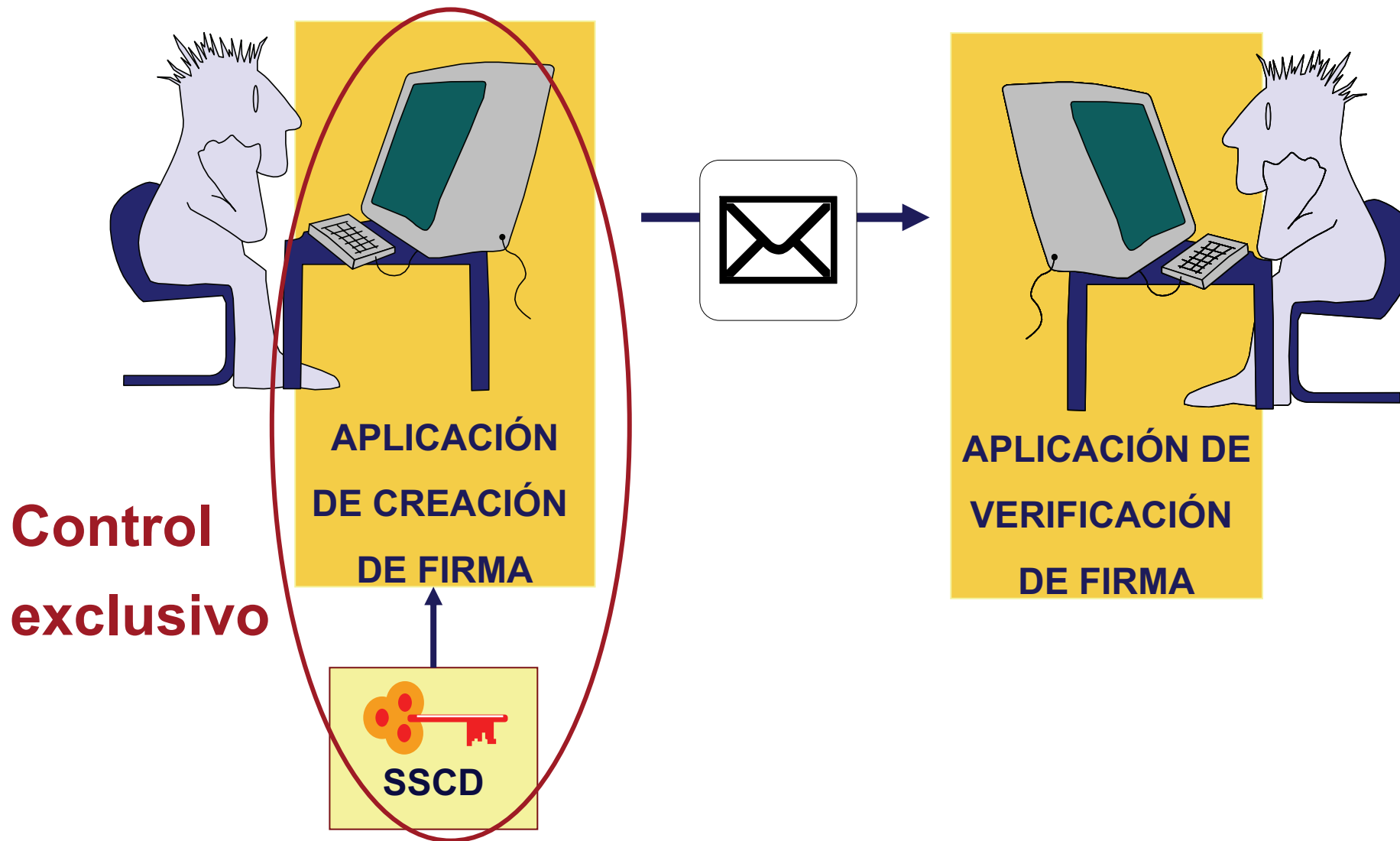
Common Methodology for Information Technology Security Evaluation (CEM)

ISO/IEC 18045. Methodology for IT Security Evaluation

Certificación de los DISPOSITIVOS de firma



Certificación de las APLICACIONES de firma



Certificación de las APLICACIONES de firma

PERFILES DE PROTECCIÓN

Aplicaciones
de creación y
verificación
de firma a
usar con el
DNI-e.

INTECO



- Seleccionar el documento para firmar.
- Seleccionar la política de firma, atributos de firma y certificado y componer los datos a ser firmados.
- Mostrar de forma no ambigua los datos a ser firmados al firmante.
- Requerir los datos de autenticación del firmante y confirmar su identidad ante el SSCD y enviar la representación de los datos a firmar (hash) al SSCD si el firmante expresa su voluntad de firmar.
- Asociar la firma-e creada por el SSCD al propio documento firmado.
- Eliminar del ámbito de control de la aplicación los datos de autenticación del firmante.

Certificación de las APLICACIONES de firma

PERFILES DE PROTECCIÓN

Aplicaciones
de creación y
verificación
de firma a
usar con el
DNI-e.

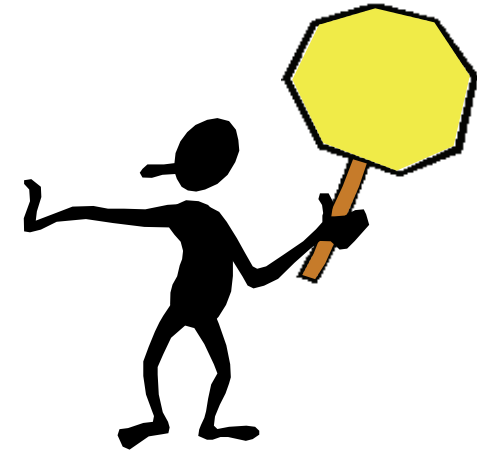
INTECO



- Seleccionar un documento firmado.
- Seleccionar la política de certificación.
- Mostrar de forma no ambigua el documento firmado y demás atributos de firma.
- Verificar la firma y mostrar el resultado de la verificación al usuario que lo solicita.

Conclusiones

- **Importancia de concretar qué tipo de firma electrónica se está utilizando.**
- **Existencia de un Esquema acreditado para la evaluación y certificación de los dispositivos seguros de creación de firma (SSCD).**
- **Conveniencia de certificar, además del SSCD, las aplicaciones de creación y verificación de firma.**



MUCHAS GRACIAS

¿PREGUNTAS?